Configuration et dépannage du chiffrement de couche réseau Cisco Contexte – 1re partie

Contenu

Introduction

Ce document discute configurer et dépanner le cryptage de réseau-couche de Cisco avec IPSec et Protocole ISAKMP (Internet Security Association and Key Management Protocol) et couvre l'information générale et la configuration de base de cryptage de réseau-couche avec IPSec et ISAKMP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations de ce document sont basées sur les versions de logiciel et matériel suivantes :

- Version de logiciel 11.2 et ultérieures de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

L'information générale et configuration de cryptage de couche réseau

La fonctionnalité de chiffrement de réseau-couche a été introduite dans la version de logiciel 11.2 de Cisco IOS®. Il fournit un mécanisme pour la transmission de données sécurisée et se compose de deux composants :

- **Authentification de routeur :** Avant de passer le trafic chiffré, deux Routeurs exécutent une authentification une fois et bi-directionnelle utilisant des clés publiques de Norme de signature numérique (DSS) pour signer des défis aléatoires.
- **Cryptage de réseau-couche :** Pour le cryptage de charge utile d'IP, l'échange de clé de Diffie-Hellman d'utilisation de Routeurs pour générer sécurisé clé de session DES(40- ou 56-bit), triple DES - 3DES(168-bit), ou l'Advanced Encryption Standard plus récent - AES(128-bit(default), ou clé 192-bit, ou 256-bit), introduite dans 12.2(13)T. De nouvelles clés de session sont générées sur une base configurable. La stratégie de chiffrement est placée par les crypto map qui emploient les Listes d'accès étendues IP pour définir que le réseau, le sous-réseau, l'hôte, ou les paires de protocole doivent être chiffré entre les Routeurs.

Fond de chiffrement

Le champ du chiffrement est concerné par maintenir des transmissions privées. La protection des transmissions sensibles a été l'accent du chiffrement dans tous beaucoup de son historique. Le cryptage est la transformation des données dans une certaine forme illisible. Son but est d'assurer l'intimité en maintenant les informations masquées de n'importe qui pour qui on ne destine pas le, même si elles peuvent voir les données cryptées. Le déchiffrement est l'inverse du cryptage : c'est la transformation des données cryptées de nouveau dans une forme intelligible.

Le cryptage et le déchiffrement exigent l'utilisation de quelques informations secrètes, habituellement visée comme une « clé ». Selon le mécanisme de chiffrement utilisé, la même clé pourrait être utilisée pour le cryptage et le déchiffrement ; tandis que pour d'autres mécanismes, les clés utilisées pour le cryptage et le déchiffrement pourraient être différents.

Une signature numérique lie un document au propriétaire d'une clé particulière, alors qu'un horodateur numérique lie un document à sa création à un moment particulier. Ces mécanismes

cryptographiques peuvent être utilisés pour contrôler l'accès à une unité de disque partagée, une installation de sécurité élevée, ou à une chaîne de télévision de pay-per-view.

Tandis que le chiffrement moderne se développe de plus en plus divers, le chiffrement est fondamentalement basé sur les problèmes il est difficile le résoudre que. Un problème peut être difficile parce que sa solution exige connaître la clé, telle que déchiffrer un message crypté ou signer un certain document numérique. Le problème peut également être difficile parce qu'il est intrinsèquement difficile de se terminer, comme trouver un message qui produit une valeur de hachage donnée.

Car le champ du chiffrement a avancé, les lignes de démarcation pour ce qui est et ce qui n'est pas chiffrement se sont estompés. Le chiffrement aujourd'hui pourrait se résumer comme étude des techniques et des applications qui dépendent de l'existence des problèmes mathématiques il est difficile le résoudre que. Les tentatives d'un cryptanalyst de compromettre les mécanismes cryptographiques, et la cryptologie est la discipline du chiffrement et de l'analyse cryptologique combinés.

Définitions

Cette section définit les termes connexes utilisés dans tout ce document.

- **Authentification :** La propriété de savoir que les données reçues sont envoyées réellement par l'expéditeur réclamé.
- **Confidentialité :** La propriété de la communication de sorte que les destinataires destinés sachent ce qui est envoyé mais les interlocuteurs fortuits ne peut pas déterminer ce qui est envoyé.
- **Norme de chiffrement de données (DES) :** Le DES utilise une méthode principale symétrique, également connue sous le nom de méthode principale secrète. Ceci signifie que si un bloc de données est chiffré avec la clé, le bloc chiffré doit être déchiffré avec la même clé, ainsi l'unité de chiffrement et le decrypter doivent utiliser la même clé. Quoique la méthode de cryptage soit connue et bien éditée, la méthode d'attaque connue de meilleur publiquement est par la force brutale. Des clés doivent être testées contre les blocs chiffrés pour voir si elles peuvent correctement les résoudre. Pendant que les processeurs deviennent plus puissants, la vie naturelle du DES s'approche de son extrémité. Par exemple, un effort coordonné utilisant la capacité de traitement supplémentaire des milliers d'ordinateurs à travers l'Internet peut trouver la clé 56-bit à un message encodé par DES en 21 jours.Le DES est validé tous les cinq ans par l'agence de Sécurité nationale des USA (NSA) pour rencontrer les buts du gouvernement des USA. L'approbation en cours expire en 1998 et le NSA a indiqué qu'ils re-ne certifieront pas le DES. Se déplacent au delà du DES, là d'autres algorithmes de chiffrement qui également n'ont aucune faiblesse connue autres que des attaques de force brutale. Pour information les informations complémentaires, voir les PAP DES 46-2 par le National Institute of Standards and Technology (NIST) .
- **Déchiffrement :** L'application inverse d'un algorithme de chiffrement aux données cryptées, restaurant de ce fait ces données sur son état d'origine et décrypté.
- **Algorithme de DSS et de signature numérique (DSA) :** Le DSA a été édité par le NIST dans le Norme de signature numérique (DSS), qui est une partie du projet de la pierre angulaire du gouvernement des États-Unis. Le DSS a été sélectionné par le NIST, en coopération avec le NSA, pour être le niveau numérique d'authentification du gouvernement des États-Unis. La norme a été émise en mai 19, 1994.

- **Cryptage :** L'application d'un algorithme spécifique aux données afin de modifier l'apparence des données la rendant incompréhensible à ceux qui ne sont pas autorisées pour voir les informations.
- **Intégrité :** La propriété de s'assurer que des données sont transmises de la source à la destination sans modification non détectée.
- **Non-répudiation :** La propriété d'un récepteur pouvant montrer que l'expéditeur de quelques données a en fait envoyé les données quoique l'expéditeur pourrait plus tard désirer refuser jamais pour avoir envoyé ces données.
- **Cryptographie à clé publique :** Le chiffrement traditionnel est basé sur l'expéditeur et le récepteur d'un message connaissant et utilisant la même clé secrète. L'expéditeur emploie la clé secrète pour chiffrer le message, et le récepteur emploie la même clé secrète pour déchiffrer le message. Cette méthode est connue en tant que le « secret-key » ou « chiffrement symétrique. » Le problème principal obtient l'expéditeur et le récepteur pour convenir sur la clé secrète sans n'importe qui d'autre qui trouve. S'ils sont dans des emplacements physiques distincts, ils doivent faire confiance à un messager, ou un système téléphonique, ou un autre support de transmission pour empêcher la divulgation de la clé secrète étant communiquée. N'importe qui qui surprend ou intercepte la clé en transit peut plus tard lire, modifier, et modifier tous les messages chiffrés ou authentifiés utilisant cette clé. La production, la transmission, et la mémoire des clés s'appelle la gestion des clés ; tous les systèmes cryptographiques doivent traiter des questions de gestion des clés. Puisque toutes les clés dans un système cryptographique de secret-key doivent demeurer secrètes, le chiffrement de secret-key a souvent la difficulté fournissant à la gestion des clés sécurisée, particulièrement dans les systèmes ouverts un grand nombre d'utilisateurs.Le concept de la cryptographie à clé publique a été introduit en 1976 par Whitfield Diffie et Martin Hellman afin de résoudre le problème de gestion des clés. Dans leur concept, chaque personne obtient une paire de clés, une appelée la clé publique et l'autre appelée la clé privée. La clé publique de chaque personne est éditée tandis que la clé privée est maintenue secrète. Le besoin de l'expéditeur et du récepteur de partager les informations secrètes est éliminé et toutes les transmissions impliquent seulement des clés publiques, et aucune clé privée n'est jamais transmise ou est partagée. N'est plus il nécessaire pour faire confiance à la voie de quelques transmissions pour être sécurisé contre l'écoute illicite ou la trahison. La seule condition requise est que des clés publiques sont associées avec leurs utilisateurs d'une manière (authentifiée) de confiance (par exemple, dans un répertoire de confiance). N'importe qui peut envoyer un message confidentiel simplement à l'aide de l'information publique, mais le message peut seulement être déchiffré avec une clé privée, qui est uniquement en possession du destinataire destiné. En outre, la cryptographie à clé publique peut être aussi bien utilisée non seulement pour l'intimité (cryptage), mais pour l'authentification (signatures numériques).
- **Signatures numériques de clé publique :** Pour signer un message, une personne exécute un calcul impliquant leur clé privée et le message elle-même. La sortie s'appelle la signature numérique et est reliée au message, qui est alors envoyé. Une deuxième personne vérifie la signature en exécutant un calcul impliquant le message, la signature prétendue, et de la première la clé publique personne. Si le résultat se tient correctement dans une relation mathématique simple, la signature est vérifiée en tant qu'étant véritable. Autrement, la signature peut être frauduleuse ou le message pourrait avoir été modifié.
- **Chiffrement à clé public :** Quand une personne souhaite envoyer un message secret à une autre personne, les premières la clé publique de deuxième personne de personne consultations dans un répertoire, l'emploie pour chiffrer le message et l'envoie. La deuxième

personne emploie alors leur clé privée pour déchiffrer le message et pour le lire. Personne qui écoute dedans ne peut déchiffrer le message. N'importe qui peut envoyer un message crypté à la deuxième personne mais seulement la deuxième personne peut le lire. Clairement, une condition requise est que personne ne peut figurer la clé privée de la clé publique correspondante.
- **Analyse du trafic :** L'analyse de l'écoulement du trafic réseau afin de déduire les informations qui sont utiles à un adversaire. Les exemples d'une telle informations sont fréquence de transmission, les identités des interlocuteurs de conversation, des tailles des paquets, des identifiants d'écoulement utilisés, et ainsi de suite.

Les informations préliminaires

Cette section discute quelques concepts de base de cryptage de réseau-couche. Il contient les aspects du cryptage pour lesquels vous devriez regarder. Au commencement, ces questions ne peuvent pas avoir du sens pour vous, mais c'est une bonne idée de les lire plus de maintenant et de se rendre compte de elles parce qu'elles sembleront plus de raisonnable après que vous ayez travaillé avec le cryptage pendant plusieurs mois.

- Il est important de noter que le cryptage se produit seulement sur la sortie d'une interface et le déchiffrement se produit seulement sur l'entrée à l'interface. Cette distinction est importante en surfaçant votre stratégie. La stratégie pour le cryptage et le déchiffrement est symétrique. Ceci signifie que cela définir un donne t'à l'autre automatiquement. Avec les crypto map et leurs Listes d'accès étendues associées, seulement la stratégie de chiffrement est explicitement définie.La stratégie de déchiffrement utilise les informations identiques, mais quand apparier des paquets, il renverse la source et les adresses de destination et les ports. Cette manière, les données est protégée dans les deux directions d'une connexion duplex. La déclaration de l'*adresse X de correspondance* dans la commande de **crypto map** est utilisée pour décrire des paquets partant d'une interface. En d'autres termes, il décrit le cryptage des paquets. Cependant, des paquets doivent également être appariés pour le déchiffrement pendant qu'ils écrivent l'interface. Ceci est fait automatiquement en traversant la liste d'accès avec la source et les adresses de destination et les ports renversés. Ceci fournit la symétrie pour la connexion. La liste d'accès indiquée par le **crypto map** devrait décrire le trafic dans une direction (sortante) seulement. Des paquets IP n'appariant pas la liste d'accès que vous définissez seront transmis mais pas chiffrés. « Refusez » dans la liste d'accès indique que ces hôtes ne devraient pas être appariés, qui signifie qu'ils ne seront pas chiffrés. « Refusez », dans ce contexte, ne signifie pas que le paquet est lâché.
- Faites attention très d'utiliser le mot « » dans les Listes d'accès étendues. Utilisant le « tout » cause votre trafic d'être relâché à moins qu'il soit dirigé à apparier « ONU-chiffrant » l'interface. En outre, avec l'IPSec dans le Logiciel Cisco IOS version 11.3(3)T, « » n'en est pas permis.
- L'utilisation du « n'importe quel » mot clé est découragée en spécifiant la source ou les adresses de destination. Spécifier « » en peut poser des problèmes avec des protocoles de routage, le Protocole NTP (Network Time Protocol), l'écho, la réponse d'écho, et le trafic de multidiffusion, car le routeur récepteur jette silencieusement ce trafic. Si « » en doit être utilisé, il devrait être précédé par « refusent » des déclarations pour le trafic qui ne doit pas être chiffré, comme le « ntp ».
- Pour épargner le temps, assurez-vous que vous pouvez **cingler le** routeur de pair avec lequel vous essayez d'avoir une association de cryptage. En outre, ayez le ping de périphériques

d'extrémité (qui dépendent d'obtenir leur trafic chiffré) avant que vous passiez trop d'heure dépannant le problème faux. En d'autres termes, assurez-vous les travaux de routage avant d'essayer pour faire **crypto**. Le pair distant peut ne pas avoir une artère pour l'interface de sortie, dans ce cas vous ne pouvez pas avoir une session de cryptage avec ce pair (vous pouvez pouvoir utiliser l'**ip unnumbered** sur cette interface série).

- Beaucoup de liens point par point BLÊMES utilisent des IP address non-routable, et le chiffrement de Logiciel Cisco IOS version 11.2 se fonde sur le Protocole ICMP (Internet Control Message Protocol) (signification qu'il utilise l'IP address de l'interface série de sortie pour l'ICMP). Ceci peut vous forcer pour utiliser l'**ip unnumbered** sur l'interface WAN. Faites toujours un **ping** et une **commande traceroute** de s'assurer que l'acheminement est en place pour les deux (chiffrer/déchiffrant) Routeurs scrutants.
- On permet à seulement deux Routeurs pour partager une clé de session de Diffie-Hellman. C'est-à-dire, un routeur ne peut pas permuter les paquets chiffrés à deux pairs utilisant la même clé de session ; chaque paire de Routeurs doit avoir une clé de session qui est un résultat d'un échange de Diffie-Hellman entre eux.
- Le moteur de chiffrement est ou dans le Cisco IOS, le Cisco IOS VIP2, ou dans le matériel le cryptage entretient l'adaptateur (ESA) sur un VIP2. Sans VIP2, le moteur de chiffrement de Cisco IOS régit la stratégie de chiffrement sur tous les ports. Sur des Plateformes utilisant le VIP2, il y a de plusieurs moteurs de chiffrement : un dans le Cisco IOS, et un sur chaque VIP2. Le moteur de chiffrement sur un VIP2 régit le cryptage sur les ports qui résident sur le panneau.
- Assurez-vous que le trafic est placé pour arriver à une interface prête à la chiffrer. Si le trafic peut d'une certaine manière arriver sur une interface autre que celle avec le **crypto map** appliqué, il est silencieusement abandonné.
- Il aide à avoir accès de console (ou remplaçant) aux deux Routeurs en faire l'échange clé ; il est possible d'obtenir le côté passif de s'arrêter tout en attendant une clé.
- **Le cfb-64** est plus efficace pour traiter que **cfb-8** en termes de chargement CPU.
- Le routeur doit exécuter l'algorithme que vous voulez utiliser avec le mode du chiffrement-feedback (CFB) que vous voulez utiliser ; les par défaut pour chaque image sont le nom d'image (tel que "56") avec **cfb-64**.
- Envisagez de changer le clé-délai d'attente. Le par défaut 30-minute est très court. Essai l'augmentant à un jour (1440 minutes).
- Le trafic IP est relâché pendant la renégociation principale chaque fois que la clé expire.
- Sélectionnez seulement le trafic que vous voulez vraiment chiffrer (ceci enregistre des cycles CPU).
- Avec le Routage à établissement de connexion à la demande (DDR), rendez l'ICMP intéressant ou il ne composera pour sortir jamais.
- Si vous voulez chiffrer le trafic autre que l'IP, utilisez un tunnel. Avec des tunnels, appliquez les crypto map à l'examen médical et aux interfaces de tunnel. Voir l'échantillon 5 : Cryptage du trafic IPX dans un pour en savoir plus de tunnel IP.
- Les deux Routeurs d'homologue de chiffrement n'ont pas besoin d'être directement connectés.
- Un routeur bas de gamme peut te donner un message « de porc CPU ». Ceci peut être ignoré parce que c'est te disant que le cryptage utilise beaucoup de ressources CPU.
- Ne placez pas les routeurs de cryptage par redondance de sorte que vous déchiffriez et re-chiffriez la CPU du trafic et de déchets. Chiffrez simplement aux deux points finaux. Voir l'échantillon 3 : Cryptage et par à un pour en savoir plus de routeur.
- Actuellement, le cryptage de l'émission et les paquets de multidiffusion n'est pas pris en

charge. Si « sécurisé » en conduisant des mises à jour soyez important pour une conception de réseaux, un protocole avec l'authentification incorporée devrait être utilisé, comme le Protocole EIGPR (Enhanced Interior Gateway Routing Protocol), le Protocole OSPF (Open Shortest Path First), ou la version 2 (RIPv2) de Protocole d'Information de Routage pour assurer l'intégrité de mise à jour.

Mises en garde

Remarque: Les mises en garde mentionnées ci-dessous tous ont été résolues.

- Un routeur de Cisco 7200 utilisant un ESA pour le cryptage ne peut pas déchiffrer un paquet au-dessous d'une clé de session et puis re-le chiffrer sous une clé de session différente. Référez-vous à l'ID de bogue Cisco CSCdj82613 (clients enregistrés seulement).
- Quand deux Routeurs sont connectés par une ligne louée chiffrée et une ligne de sauvegarde RNIS, si la ligne louée chute, la liaison RNIS est soulevée bien. Cependant, quand la ligne louée se réactive de nouveau, le routeur qui a placé l'appel RNIS tombe en panne. Référez-vous à l'ID de bogue Cisco CSCdj00310 (clients enregistrés seulement).
- Pour le Routeurs de la gamme Cisco 7500 avec de plusieurs VIPs, si un **crypto map** est appliqué même à une interface de n'importe quel VIP, un ou plusieurs VIPs tombent en panne. Référez-vous à l'ID de bogue Cisco CSCdi88459 (clients enregistrés seulement).
- Pour le Routeurs de la gamme Cisco 7500 avec un VIP2 et un ESA, la commande **crypto de carte d'exposition** n'affiche pas la sortie à moins que l'utilisateur soit au port de console. Référez-vous à l'ID de bogue Cisco CSCdj89070 (clients enregistrés seulement).

Configuration de chiffrement de réseau-couche de Cisco IOS

Les configurations Cisco IOS fonctionnantes d'échantillon dans ce document ont été livré directement des routeurs de laboratoire. La seule modification apportée à eux était la suppression des configurations d'interface indépendantes. Tout les contenu ici est provenu librement des ressources disponibles sur l'Internet ou dans la section Informations connexes à la fin de ce document.

Toutes les configurations d'échantillon dans ce document sont de Logiciel Cisco IOS version 11.3. Il y avait plusieurs modifications des commandes de Logiciel Cisco IOS version 11.2, telles que l'ajout des mots suivants :

- DSS dans certaines des commandes de configuration principales.
- Cisco dans une partie des **commandes show** et du **crypto map** commande de distinguer le chiffrement de propriété industrielle de Cisco (comme trouvé dans le Logiciel Cisco IOS version 11.2 et plus tard) et l'IPSec qui est dans le Logiciel Cisco IOS version 11.3(2)T.

Remarque: Les adresses IP utilisées dans ces exemples de configuration ont été choisies aléatoirement dans le laboratoire de Cisco et sont destinées pour être complètement génériques.

Étape 1 : Générez manuellement les paires de clés de DSS

Une paire de clés de DSS (un public et une clé privée) doit être manuellement générée sur chaque routeur participant à la session de cryptage. En d'autres termes, chaque routeur doit avoir ses propres clés de DSS afin de participer. Une engine de cryptage peut avoir seulement un DSS

principal qui l'identifie seulement. Le mot clé « DSS » a été ajouté dans le Logiciel Cisco IOS version 11.3 afin de distinguer le DSS des clés RSA. Vous pouvez spécifier n'importe quel nom pour les propres clés du DSS du routeur (bien que, il est recommandé d'utiliser le nom de hôte du routeur). Sur une CPU moins puissante (telle que la gamme Cisco 2500), la génération de paire de clés prend environ 5 secondes ou moins.

Le routeur génère une paire de clés :

- Une clé publique (qui plus tard est envoyée aux Routeurs participant aux sessions de cryptage).
- Une clé privée (qui n'est pas vue ni est permutée avec n'importe qui d'autre ; en fait, il est enregistré dans une partie indépendant de NVRAM qui ne peut pas être visualisé).

Une fois que la paire de clés du DSS du routeur a été générée, elle est seulement associée avec le moteur de chiffrement dans ce routeur. La génération de paire de clés est affichée dans l'exemple de sortie de commande ci-dessous.

```
dial-5(config)#crypto key generate dss dial5 Generating DSS keys .... [OK] dial-5#show crypto key mypubkey dss crypto public-key dial5 05679919 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145 quit dial-5#show crypto engine configuration slot: 0 engine name: dial5 engine type: software serial number: 05679919 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 43 input queue bot: 43 input queue count: 0 dial-5#
```

Puisque vous pouvez générer seulement une paire de clés qui identifie le routeur, vous pouvez remplacer votre clé d'origine et devoir renvoyer votre clé publique avec chaque routeur dans l'association de cryptage. Ceci est affiché dans l'exemple de sortie de commande ci-dessous :

```
StHelen(config)#crypto key generate dss barney % Generating new DSS keys will require re-exchanging public keys with peers who already have the public key named barney! Generate new DSS keys? [yes/no]: yes Generating DSS keys .... [OK] StHelen(config)# Mar 16 12:13:12.851: Crypto engine 0: create key pairs.
```

Étape 2 : Permutez manuellement les clés publiques de DSS avec des pairs (hors bande)

Générer la propre paire de clés du DSS du routeur est la première étape en établissant une association de session de cryptage. L'étape suivante est de permuter des clés publiques avec chaque autre routeur. Vous pouvez introduire ces clés publiques manuellement en écrivant d'abord la **crypto** commande de **mypubkey d'exposition** d'afficher la clé publique du DSS du routeur. Vous alors permutez ces clés publiques (par l'intermédiaire de l'email, par exemple) et, avec la **crypto** commande **principale de DSS de pubkey-chaîne**, coupez-collez la clé publique de votre routeur de pair dans le routeur.

Vous pouvez également utiliser la **crypto** commande **principale de DSS d'échange** d'avoir les clés publiques d'échange de Routeurs automatiquement. Si vous utilisez la méthode automatisée, assurez-vous qu'il n'y a aucune déclaration de **crypto map** sur les interfaces utilisées pour l'échange clé. **Une clé de debug crypto** est utile ici.

Remarque: C'est une bonne idée **de cingler** votre pair avant d'essayer pour permuter des clés.

```
Loser#ping 19.19.19.20 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds: !!!!! Loser(config)#crypto key exchange dss passive Enter escape character to abort if connection does not complete. Wait for connection from peer[confirm] Waiting .... StHelen(config)#crypto key exchange dss 19.19.19.19 barney Public key for barney: Serial Number 05694352 Fingerprint 309E D1DE B6DA 5145 D034 Wait for peer to send a key[confirm] Public key for barney: Serial Number 05694352 Fingerprint 309E D1DE B6DA 5145 D034
```

```
Add this public key to the configuration? [yes/no]:yes Mar 16 12:16:55.343: CRYPTO-KE: Sent 2
bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2
bytes. Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes. Mar 16 12:16:45.099: CRYPTO-KE: Received 4
bytes. Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:45.103: CRYPTO-KE:
Received 6 bytes. Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:45.107: CRYPTO-
KE: Received 50 bytes. Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes. Send peer a key in
return[confirm] Which one? fred? [yes]: Public key for fred: Serial Number 02802219 Fingerprint
2963 05F9 ED55 576D CF9D Waiting .... Public key for fred: Serial Number 02802219 Fingerprint
2963 05F9 ED55 576D CF9D Add this public key to the configuration? [yes/no]: Loser(config)# Mar
16 12:16:55.339: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes. Mar 16
12:16:55.343: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes. Mar 16
12:16:55.347: CRYPTO-KE: Sent 64 bytes. Loser(config)# Mar 16 12:16:56.083: CRYPTO-KE: Received
4 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.087: CRYPTO-KE:
Received 4 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.091: CRYPTO-
KE: Received 52 bytes. Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes. Add this public key to
the configuration? [yes/no]: yes StHelen(config)#^Z StHelen#
```

Maintenant que des clés publiques de DSS ont été permutées, assurez-vous que les deux Routeurs ont des clés publiques de chacun et qu'ils sont assortis, suivant les indications de la sortie de commande ci-dessous.

```
Loser#show crypto key mypubkey dss crypto public-key fred 02802219 79CED212 AF191D29 702A9301
B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402
D443F68D 93487F7E 5ABE182E quit Loser#show crypto key pubkey-chain dss crypto public-key barney
05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED 732EA43D
484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341 quit -------- StHelen#show crypto
key mypubkey dss crypto public-key barney 05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A
3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477
91810341 quit StHelen#show crypto key pubkey-chain dss crypto public-key fred 02802219 79CED212
AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5
679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit
```

Échantillon 1 : Configuration Cisco IOS pour la liaison dédiée

Après que les clés de DSS aient été générées sur chaque routeur et les clés publiques de DSS ont été permutées, la commande de **crypto map** peut être appliquée à l'interface. La crypto session commence en générant le trafic qui apparie la liste d'accès utilisée par les crypto map.

```
Loser#write terminal Building configuration... Current configuration: ! ! Last configuration
change at 13:01:18 UTC Mon Mar 16 1998 ! NVRAM config last updated at 13:03:02 UTC Mon Mar 16
1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption !
hostname Loser ! enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no ip domain-
lookup crypto map oldstyle 10 set peer barney match address 133 ! crypto key pubkey-chain dss
named-key barney serial-number 05694352 key-string B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A
3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477
91810341 quit ! interface Ethernet0 ip address 40.40.40.41 255.255.255.0 no ip mroute-cache !
interface Serial0 ip address 18.18.18.18 255.255.255.0 encapsulation ppp no ip mroute-cache
shutdown ! interface Serial1 ip address 19.19.19.19 255.255.255.0 encapsulation ppp no ip
mroute-cache clockrate 2400 no cdp enable crypto map oldstyle ! ip default-gateway 10.11.19.254
ip classless ip route 0.0.0.0 0.0.0.0 19.19.19.20 access-list 133 permit ip 40.40.40.0 0.0.0.255
30.30.30.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport input all line
vty 0 4 password ww login ! end Loser# ------------------------- StHelen#write terminal
Building configuration... Current configuration: ! ! Last configuration change at 13:03:05 UTC
Mon Mar 16 1998 ! NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998 ! version 11.3
service timestamps debug datetime msec no service password-encryption ! hostname StHelen ! boot
system flash c2500-is56-l enable password ww ! partition flash 2 8 8 ! no ip domain-lookup
crypto map oldstyle 10 set peer fred match address 144 ! crypto key pubkey-chain dss named-key
fred serial-number 02802219 key-string 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8
05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit !
! interface Ethernet0 ip address 30.30.30.31 255.255.255.0 ! interface Ethernet1 no ip address
shutdown ! interface Serial0 no ip address encapsulation x25 no ip mroute-cache shutdown !
interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation ppp no ip mroute-cache
load-interval 30 compress stac no cdp enable crypto map oldstyle ! ip default-gateway
```

```
10.11.19.254 ip classless ip route 0.0.0.0 0.0.0.0 19.19.19.19 access-list 144 permit ip
30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport
input all line vty 0 4 password ww login ! end StHelen#
```

Échantillon 2 : Configuration Cisco IOS pour le relais de trame multipoint

L'exemple de sortie de commande suivant a été pris du routeur concentrateur.

```
Loser#write terminal Building configuration... Current configuration: ! ! Last configuration
change at 10:45:20 UTC Wed Mar 11 1998 ! NVRAM config last updated at 18:28:27 UTC Tue Mar 10
1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption !
hostname Loser ! enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no ip domain-
lookup ! crypto map oldstuff 10 set peer barney match address 133 crypto map oldstuff 20 set
peer wilma match address 144 ! crypto key pubkey-chain dss named-key barney serial-number
05694352 key-string 1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D quit named-key wilma
serial-number 01496536 key-string C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70
7B29279C E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939 quit ! crypto
cisco pregen-dh-pairs 5 ! crypto cisco key-timeout 1440 ! interface Ethernet0 ip address
190.190.190.190 255.255.255.0 no ip mroute-cache ! interface Serial1 ip address 19.19.19.19
255.255.255.0 encapsulation frame-relay no ip mroute-cache clockrate 500000 crypto map oldstuff
! ! ip default-gateway 10.11.19.254 ip classless ip route 200.200.200.0 255.255.255.0
19.19.19.20 ip route 210.210.210.0 255.255.255.0 19.19.19.21 access-list 133 permit ip
190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255 access-list 144 permit ip 190.190.190.0
0.0.0.255 210.210.210.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport
input all line vty 0 4 password ww login ! end Loser#
```

L'exemple de sortie de commande suivant a été pris du site distant R.

```
WAN-2511a#write terminal Building configuration... Current configuration: ! version 11.3 no
service password-encryption ! hostname WAN-2511a ! enable password ww ! no ip domain-lookup !
crypto map mymap 10 set peer fred match address 133 ! crypto key pubkey-chain dss named-key fred
serial-number 02802219 key-string 56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592
021B295D D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436 quit !
interface Ethernet0 ip address 210.210.210.210 255.255.255.0 shutdown ! interface Serial0 ip
address 19.19.19.21 255.255.255.0 encapsulation frame-relay no fair-queue crypto map mymap ! ip
default-gateway 10.11.19.254 ip classless ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255 ! line con 0 exec-
timeout 0 0 line 1 no exec transport input all line 2 16 no exec line aux 0 line vty 0 4
password ww login ! end WAN-2511a#
```

L'exemple de sortie de commande suivant a été pris du site distant B.

```
StHelen#write terminal Building configuration... Current configuration: ! ! Last configuration
change at 19:00:34 UTC Tue Mar 10 1998 ! NVRAM config last updated at 18:48:39 UTC Tue Mar 10
1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption !
hostname StHelen ! boot system flash c2500-is56-l enable password ww ! partition flash 2 8 8 !
no ip domain-lookup ! crypto map wabba 10 set peer fred match address 144 ! crypto key pubkey-
chain dss named-key fred serial-number 02802219 key-string 56841777 4F27A574 5005E0F0 CF3C33F5
C6AAD000 5518A8FF 7422C592 021B295D D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D
0256EFF5 0EE89436 quit ! interface Ethernet0 ip address 200.200.200.200 255.255.255.0 !
interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation frame-relay no ip mroute-
cache crypto map wabba ! ip default-gateway 10.11.19.254 ip classless ip route 190.190.190.0
255.255.255.0 19.19.19.19 access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0
0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport input all line vty 0 4 password ww
login ! end StHelen#
```

L'exemple de sortie de commande suivant a été pris du commutateur de Relais de trames.

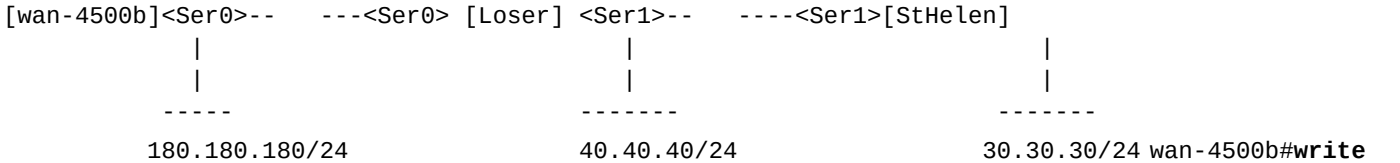
```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
```

```
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 100
!
interface Serial1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 100 interface Serial0 200
 frame-relay route 300 interface Serial2 200
!
interface Serial2
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 300
!
```

Échantillon 3 : Cryptage et par à un routeur

Les Routeurs de pair ne doivent pas être un saut loin. Vous pouvez créer une session scrutante avec un routeur distant. Dans l'exemple suivant, le but est de chiffrer tout le trafic réseau entre 180.180.180.0/24 et 40.40.40.0/24 et entre 180.180.180.0/24 et 30.30.30.0/24. Il n'y a aucun souci avec le trafic de chiffrage entre 40.40.40.0/24 et 30.30.30.0/24.

Le routeur wan-4500b a une association de session de cryptage avec le perdant et également avec StHelen. En chiffrant le trafic du segment d'Ethernets wan-4500b au segment des Ethernets de StHelen, vous évitez l'étape inutile de déchiffrement au perdant. Le perdant transmet simplement le trafic chiffré à l'interface série de StHelen, où elle est déchiffrée. Ceci réduit le retard du trafic pour les paquets IP et les cycles CPU sur le perdant de routeur. D'une manière primordiale, il augmente considérablement la Sécurité du système, puisqu'une oreille indiscrète au perdant ne peut pas lire le trafic. Si le perdant déchiffraient le trafic, il y aurait une occasion que les données déchiffrées pourraient être détournées.




```
wan-4500b#write terminal Building configuration... Current configuration: ! version 11.3 no service password-encryption ! hostname wan-4500b ! enable password 7 111E0E ! username cse password 0 ww no ip domain-lookup ! crypto map toworld 10 set peer loser match address 133 crypto map toworld 20 set peer sthelen match address 144 ! crypto key pubkey-chain dss named-key loser serial-number 02802219 key-string F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit named-key sthelen serial-number 05694352 key-string 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit ! interface Ethernet0 ip address 180.180.180.180 255.255.255.0 ! interface Serial0 ip address 18.18.18.19 255.255.255.0 encapsulation ppp crypto map toworld ! router rip network 18.0.0.0
```

network 180.180.0.0 ! ip classless ip route 0.0.0.0 0.0.0.0 30.30.30.31 ip route 171.68.118.0 255.255.255.0 10.11.19.254 access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0 0.0.0.255 access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 password 7 044C1C line vty 0 4 login local ! end wan-4500b# ---------- Loser#**write terminal** Building configuration... Current configuration: ! ! Last configuration change at 11:01:54 UTC Wed Mar 18 1998 ! NVRAM config last updated at 11:09:59 UTC Wed Mar 18 1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname Loser ! enable secret 5 1AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no ip domain-lookup ip host StHelen.cisco.com 19.19.19.20 ip domain-name cisco.com ! crypto map towan 10 set peer wan match address 133 ! crypto key pubkey-chain dss named-key wan serial-number 07365004 key-string A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit ! interface Ethernet0 ip address 40.40.40.40 255.255.255.0 no ip mroute-cache ! interface Serial0 ip address 18.18.18.18 255.255.255.0 encapsulation ppp no ip mroute-cache clockrate 64000 crypto map towan ! interface Serial1 ip address 19.19.19.19 255.255.255.0 encapsulation ppp no ip mroute-cache priority-group 1 clockrate 64000 ! ! router rip network 19.0.0.0 network 18.0.0.0 network 40.0.0.0 ! ip default-gateway 10.11.19.254 ip classless access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport input all line vty 0 4 password ww login ! end Loser# ---------- StHelen#**write terminal** Building configuration... Current configuration: ! ! Last configuration change at 11:13:18 UTC Wed Mar 18 1998 ! NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname StHelen ! boot system flash c2500-is56-l enable password ww ! partition flash 2 8 8 ! no ip domain-lookup ! crypto map towan 10 set peer wan match address 144 ! crypto key pubkey-chain dss named-key wan serial-number 07365004 key-string A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit ! interface Ethernet0 no ip address ! interface Ethernet1 ip address 30.30.30.30 255.255.255.0 ! interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation ppp no ip mroute-cache load-interval 30 crypto map towan ! router rip network 30.0.0.0 network 19.0.0.0 ! ip default-gateway 10.11.19.254 ip classless access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport input all line vty 0 4 password ww login ! end StHelen# ---------- wan-4500b#**show crypto cisco algorithms** des cfb-64 40-bit-des cfb-64 wan-4500b#**show crypto cisco key-timeout** Session keys will be re-negotiated every 30 minutes wan-4500b#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 0 wan-4500b#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 Serial0 18.18.18.19 set DES_56_CFB64 1683 1682 5 Serial0 18.18.18.19 set DES_56_CFB64 1693 1693 wan-4500b#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Serial0 18.18.18.19 52 wan-4500b#**show crypto engine configuration** slot: 0 engine name: wan engine type: software serial number: 07365004 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 303 input queue bot: 303 input queue count: 0 wan-4500b#**show crypto key mypubkey dss** crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit wan-4500b#**show crypto key pubkey-chain dss** crypto public-key loser 02802219 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit crypto public-key sthelen 05694352 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit wan-4500b#**show crypto map interface serial 1** No crypto maps found. wan-4500b#**show crypto map** Crypto Map "toworld" 10 cisco Connection Id = 1 (1 established, 0 failed) Peer = loser PE = 180.180.180.0 UPE = 40.40.40.0 Extended IP access list 133 access-list 133 permit ip source: addr = 180.180.180.0/0.0.0.255 dest: addr = 40.40.40.0/0.0.0.255 Crypto Map "toworld" 20 cisco Connection Id = 5 (1 established, 0 failed) Peer = sthelen PE = 180.180.180.0 UPE = 30.30.30.0 Extended IP access list 144 access-list 144 permit ip source: addr = 180.180.180.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255 wan-4500b# ---------- Loser#**show crypto cisco algorithms** des cfb-64 des cfb-8 40-bit-des cfb-64 40-bit-des cfb-8 Loser#**show crypto cisco key-timeout** Session keys will be re-negotiated every 30 minutes Loser#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 10 Loser#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 61 Serial0 18.18.18.18 set DES_56_CFB64 1683 1682 Loser#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Serial0 18.18.18.18 1 Serial1 19.19.19.19 90 Loser#**show crypto engine configuration** slot: 0 engine name: loser engine type: software serial number: 02802219 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 235 input queue bot: 235 input queue count: 0 Loser#**show crypto key mypubkey dss** crypto public-key loser 02802219 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4

```
6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit Loser#show crypto
key pubkey-chain dss crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3
B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB
86269A5B quit Loser#show crypto map interface serial 1 No crypto maps found. Loser#show crypto
map Crypto Map "towan" 10 cisco Connection Id = 61 (0 established, 0 failed) Peer = wan PE =
40.40.40.0 UPE = 180.180.180.0 Extended IP access list 133 access-list 133 permit ip source:
addr = 40.40.40.0/0.0.0.255 dest: addr = 180.180.180.0/0.0.0.255 Loser# ----------------------
---------------- StHelen#show crypto cisco algorithms des cfb-64 StHelen#show crypto cisco key-
timeout Session keys will be re-negotiated every 30 minutes StHelen#show crypto cisco pregen-dh-
pairs Number of pregenerated DH pairs: 10 StHelen#show crypto engine connections active ID
Interface IP-Address State Algorithm Encrypt Decrypt 58 Serial1 19.19.19.20 set DES_56_CFB64
1694 1693 StHelen#show crypto engine connections dropped-packet Interface IP-Address Drop Count
Ethernet0 0.0.0.0 1 Serial1 19.19.19.20 80 StHelen#show crypto engine configuration slot: 0
engine name: sthelen engine type: software serial number: 05694352 platform: rp crypto engine
crypto lib version: 10.0.0 Encryption Process Info: input queue top: 220 input queue bot: 220
input queue count: 0 StHelen#show crypto key mypubkey dss crypto public-key sthelen 05694352
5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10 A23848CA 46003A94
2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit StHelen#show crypto key pubkey-chain
dss crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A
F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit
StHelen#show crypto map interface serial 1 Crypto Map "towan" 10 cisco Connection Id = 58 (1
established, 0 failed) Peer = wan PE = 30.30.30.0 UPE = 180.180.180.0 Extended IP access list
144 access-list 144 permit ip source: addr = 30.30.30.0/0.0.0.255 dest: addr =
180.180.180.0/0.0.0.255 StHelen#show crypto map Crypto Map "towan" 10 cisco Connection Id = 58
(1 established, 0 failed) Peer = wan PE = 30.30.30.0 UPE = 180.180.180.0 Extended IP access list
144 access-list 144 permit ip source: addr = 30.30.30.0/0.0.0.255 dest: addr =
180.180.180.0/0.0.0.255 StHelen#
```

Échantillon 4 : Crypto avec le DDR

Puisque le Cisco IOS se fonde sur l'ICMP pour établir des sessions de cryptage, le trafic d'ICMP doit être classifié en tant que « intéressant » dans la liste d'appels en faire le cryptage au-dessus d'un lien DDR.

Remarque: Le compactage fonctionne dans le Logiciel Cisco IOS version 11.3, mais il n'est pas très utile pour des données chiffrées. Puisque les données cryptées sont assez à l'air aléatoire, le compactage ralentit seulement des choses vers le bas. Mais vous pouvez laisser la caractéristique en fonction pour le trafic non chiffré.

Dans certaines situations, vous voudrez l'Accès direct secouru au même routeur. Par exemple, il est utile quand les utilisateurs veulent se protéger contre la panne d'un lien particulier dans leurs réseaux BLÊMES. Si deux interfaces vont au même pair, le même crypto map peut être utilisé sur les deux interfaces. L'Interface de sauvegarde doit être utilisée pour que cette caractéristique fonctionne correctement. Si une conception de sauvegarde a un cadran de routeur dans une case différente, différents crypto map devraient être créés et les pairs être placés en conséquence. De nouveau, la **commande backup interface** devrait être utilisée.

```
dial-5#write terminal Building configuration... Current configuration: ! version 11.3 no service
password-encryption service udp-small-servers service tcp-small-servers ! hostname dial-5 ! boot
system c1600-sy56-l 171.68.118.83 enable secret 5 $1$oNe1wDbhBdcN6x9Y5gfuMjqh10 ! username dial-
6 password 0 cisco isdn switch-type basic-ni1 ! crypto map dial6 10 set peer dial6 match address
133 ! crypto key pubkey-chain dss named-key dial6 serial-number 05679987 key-string 753F71AB
E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82 2BC91236 13DC4AA8 7EC5B48C
D276E5FE 0D093014 6D3061C5 03158820 B609CA7C quit ! interface Ethernet0 ip address 20.20.20.20
255.255.255.0 ! interface BRI0 ip address 10.10.10.11 255.255.255.0 encapsulation ppp no ip
mroute-cache load-interval 30 dialer idle-timeout 9000 dialer map ip 10.10.10.10 name dial-6
4724118 dialer hold-queue 40 dialer-group 1 isdn spid1 919472417100 4724171 isdn spid2
919472417201 4724172 compress stac ppp authentication chap ppp multilink crypto map dial6 ! ip
classless ip route 40.40.40.0 255.255.255.0 10.10.10.10 access-list 133 permit ip 20.20.20.0
0.0.0.255 40.40.40.0 0.0.0.255 dialer-list 1 protocol ip permit ! line con 0 exec-timeout 0 0
```

line vty 0 4 password ww login ! end dial-5# ---------- dial-6#**write terminal** Building configuration... Current configuration: ! version 11.3 no service password-encryption service udp-small-servers service tcp-small-servers ! hostname dial-6 ! boot system c1600-sy56-l 171.68.118.83 enable secret 5 1VdPYuA/BIVeEm9UAFEm.PPJFc. ! username dial-5 password 0 cisco no ip domain-lookup isdn switch-type basic-ni1 ! crypto map dial5 10 set peer dial5 match address 144 ! crypto key pubkey-chain dss named-key dial5 serial-number 05679919 key-string 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145 quit ! ! interface Ethernet0 ip address 40.40.40.40 255.255.255.0 ! interface BRI0 ip address 10.10.10.10 255.255.255.0 encapsulation ppp no ip mroute-cache dialer idle-timeout 9000 dialer map ip 10.10.10.11 name dial-5 4724171 dialer hold-queue 40 dialer load-threshold 5 outbound dialer-group 1 isdn spid1 919472411800 4724118 isdn spid2 919472411901 4724119 compress stac ppp authentication chap ppp multilink crypto map dial5 ! ip classless ip route 20.20.20.0 255.255.255.0 10.10.10.11 access-list 144 permit ip 40.40.40.0 0.0.0.255 20.20.20.0 0.0.0.255 dialer-list 1 protocol ip permit ! line con 0 exec-timeout 0 0 line vty 0 4 password ww login ! end dial-6#

Échantillon 5 : Cryptage du trafic IPX dans un tunnel IP

Dans cet exemple, le trafic IPX dans un tunnel IP est chiffré.

Remarque: Seulement le trafic dans ce tunnel (IPX) est chiffré. Tout autre trafic IP est conservé.

WAN-2511a#**write terminal** Building configuration... Current configuration: ! version 11.2 no service password-encryption no service udp-small-servers no service tcp-small-servers ! hostname WAN-2511a ! enable password ww ! no ip domain-lookup ipx routing 0000.0c34.aa6a ! crypto public-key wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit ! crypto map wan2516 10 set peer wan2516 match address 133 ! ! interface Loopback1 ip address 50.50.50.50 255.255.255.0 ! interface Tunnel1 no ip address ipx network 100 tunnel source 50.50.50.50 tunnel destination 60.60.60.60 crypto map wan2516 ! interface Ethernet0 ip address 40.40.40.40 255.255.255.0 ipx network 600 ! interface Serial0 ip address 20.20.20.21 255.255.255.0 encapsulation ppp no ip mroute-cache crypto map wan2516 ! interface Serial1 no ip address shutdown ! ip default-gateway 10.11.19.254 ip classless ip route 0.0.0.0 0.0.0.0 20.20.20.20 access-list 133 permit ip host 50.50.50.50 host 60.60.60.60 ! line con 0 exec-timeout 0 0 password ww login line 1 16 line aux 0 password ww login line vty 0 4 password ww login ! end WAN-2511a# ---------- WAN-2516a#**write terminal** Building configuration... Current configuration: ! version 11.2 no service pad no service password-encryption service udp-small-servers service tcp-small-servers ! hostname WAN-2516a ! enable password ww ! no ip domain-lookup ipx routing 0000.0c3b.cc1e ! crypto public-key wan2511 01496536 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553 quit ! crypto map wan2511 10 set peer wan2511 match address 144 ! ! hub ether 0 1 link-test auto-polarity ! ! <other hub interfaces snipped> ! hub ether 0 14 link-test auto-polarity ! interface Loopback1 ip address 60.60.60.60 255.255.255.0 ! interface Tunnel1 no ip address ipx network 100 tunnel source 60.60.60.60 tunnel destination 50.50.50.50 crypto map wan2511 ! interface Ethernet0 ip address 30.30.30.30 255.255.255.0 ipx network 400 ! interface Serial0 ip address 20.20.20.20 255.255.255.0 encapsulation ppp clockrate 2000000 crypto map wan2511 ! interface Serial1 no ip address shutdown ! interface BRI0 no ip address shutdown ! ip default-gateway 20.20.20.21 ip classless ip route 0.0.0.0 0.0.0.0 20.20.20.21 access-list 144 permit ip host 60.60.60.60 host 50.50.50.50 access-list 188 permit gre any any ! line con 0 exec-timeout 0 0 password ww login line aux 0 password ww login modem InOut transport input all flowcontrol hardware line vty 0 4 password ww login ! end WAN-2516a# ---------- WAN-2511a#**show ipx route** Codes: C - Connected primary network, c - Connected secondary network S - Static, F - Floating static, L - Local (internal), W - IPXWAN R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate s - seconds, u - uses 3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed. No default route known. C 100 (TUNNEL), Tu1 C 600 (NOVELL-ETHER), Et0 R 400 [151/01] via 100.0000.0c3b.cc1e, 24s, Tu1 WAN-2511a#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 Serial0 20.20.20.21 set DES_56_CFB64 207 207 WAN-2511a#**ping 400.0000.0c3b.cc1e** Translating "400.0000.0c3b.cc1e" Type escape sequence to abort. Sending 5, 100-byte IPX cisco Echoes to 400.0000.0c3b.cc1e, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/48 ms WAN-2511a#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 Serial0 20.20.20.21 set DES_56_CFB64 212 212 WAN-2511a#**ping 30.30.30.30** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to

```
30.30.30.30, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip
min/avg/max = 4/5/8 ms WAN-2511a#show crypto engine connections active ID Interface IP-Address
State Algorithm Encrypt Decrypt 1 Serial0 20.20.20.21 set DES_56_CFB64 212 212 WAN-2511a#
```

Échantillon 6 : Chiffrer des tunnels L2F

Dans cet exemple, chiffrer seulement le trafic L2F pour se connecter d'utilisateurs est tenté. Ici, « user@cisco.com » appelle le serveur d'accès de réseau local (NAS) a nommé "DEMO2" à leur ville et l'obtient percé un tunnel au CD de passerelle domestique. Tout le trafic DEMO2 (avec cela d'autres appelants L2F) est chiffré. Puisque L2F utilise le port UDP 1701, c'est comment la liste d'accès est construite, déterminant quel trafic est chiffré.

Remarque: Si l'association de cryptage n'est pas déjà d'installer, la signification de l'appelant est la première personne à appeler dedans et créer le tunnel L2F, l'appelant peut obtenir relâché en raison du retard à installer l'association de cryptage. Ceci peut ne pas se produire sur des Routeurs avec assez de puissance CPU. En outre, vous pouvez vouloir augmenter le **keytimeout** de sorte que le cryptage ait installé et le démontage se produise seulement pendant des heures creuses.

L'exemple de sortie de commande suivant a été pris du NAS distant.

```
DEMO2#write terminal Building configuration... Current configuration: ! version 11.2 no service
password-encryption no service udp-small-servers no service tcp-small-servers ! hostname DEMO2 !
enable password ww ! username NAS1 password 0 SECRET username HomeGateway password 0 SECRET no
ip domain-lookup vpdn enable vpdn outgoing cisco.com NAS1 ip 20.20.20.20 ! crypto public-key
wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit ! crypto map vpdn
10 set peer wan2516 match address 133 ! crypto key-timeout 1440 ! interface Ethernet0 ip address
40.40.40.40 255.255.255.0 ! interface Serial0 ip address 20.20.20.21 255.255.255.0 encapsulation
ppp no ip mroute-cache crypto map vpdn ! interface Serial1 no ip address shutdown ! interface
Group-Async1 no ip address encapsulation ppp async mode dedicated no peer default ip address no
cdp enable ppp authentication chap pap group-range 1 16 ! ip default-gateway 10.11.19.254 ip
classless ip route 0.0.0.0 0.0.0.0 20.20.20.20 access-list 133 permit udp host 20.20.20.21 eq
1701 host 20.20.20.20 eq 1701 ! ! line con 0 exec-timeout 0 0 password ww login line 1 16 modem
InOut transport input all speed 115200 flowcontrol hardware line aux 0 login local modem InOut
transport input all flowcontrol hardware line vty 0 4 password ww login ! end DEMO2#
```

L'exemple de sortie de commande suivant a été pris de la passerelle domestique.

```
CD#write terminal Building configuration... Current configuration: ! version 11.2 no service pad
no service password-encryption service udp-small-servers service tcp-small-servers ! hostname CD
! enable password ww ! username NAS1 password 0 SECRET username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco no ip domain-lookup vpdn enable vpdn incoming NAS1
HomeGateway virtual-template 1 ! crypto public-key wan2511 01496536 C8EA7C21 DF3E48F5 C6C069DB
3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1
E2FCDC05 545E0529 9B3C9553 quit ! crypto key-timeout 1440 ! crypto map vpdn 10 set peer wan2511
match address 144 ! ! hub ether 0 1 link-test auto-polarity ! interface Loopback0 ip address
70.70.70.1 255.255.255.0 ! interface Ethernet0 ip address 30.30.30.30 255.255.255.0 ! interface
Virtual-Template1 ip unnumbered Loopback0 no ip mroute-cache peer default ip address pool
default ppp authentication chap ! interface Serial0 ip address 20.20.20.20 255.255.255.0
encapsulation ppp clockrate 2000000 crypto map vpdn ! interface Serial1 no ip address shutdown !
interface BRI0 no ip address shutdown ! ip local pool default 70.70.70.2 70.70.70.77 ip default-
gateway 20.20.20.21 ip classless ip route 0.0.0.0 0.0.0.0 20.20.20.21 access-list 144 permit udp
host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701 ! line con 0 exec-timeout 0 0 password ww
login line aux 0 password ww login modem InOut transport input all flowcontrol hardware line vty
0 4 password ww login ! end
```

Dépannage

Il est généralement le meilleur de commencer chaque session de dépannage en recueillant des

informations utilisant les **commandes show** suivantes. Un astérisque (*) indique une commande particulièrement utile. Veuillez voir également le dépannage de sécurité IP - Comprenant et utilisant des commandes de débogage pour information les informations complémentaires.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

Commandes	
affichez les cryptos algorithmes de Cisco	affichez le crypto clé-délai d'attente de Cisco
affichez les cryptos pregen-CAD-paires de Cisco	* connexions de show crypto engine actives
relâcher-paquet de connexions de show crypto engine	configuration de show crypto engine
DSS de mypubkey de show crypto key	* DSS de pubkey-chaîne de show crypto key
affichez l'interface série 1 d'interface de crypto map	* affichez le crypto map
debug crypto engine	* sess de debug crypto
mettez au point la clé de cri	effacez la crypto connexion
crypto mise à zéro	aucune crypto clé publique

- **affichez les cryptos algorithmes de Cisco**- Vous devez activer tous les algorithmes de Norme de chiffrement de données (DES) qui sont utilisés pour communiquer avec n'importe quel autre routeur de cryptage de pair. Si vous n'activez pas un algorithme DES, vous ne pourrez pas utiliser cet algorithme, même si vous essayez d'assigner l'algorithme à un **crypto map** à une date ultérieure.Si votre routeur tente d'installer une session de communication chiffrée avec un routeur de pair, et les deux Routeurs n'ont pas le même algorithme DES activé aux deux extrémités, la session chiffrée échoue. Si au moins un algorithme commun DES est activé aux deux extrémités, la session chiffrée peut poursuivre.**Remarque:** Le mot supplémentaire Cisco apparaît dans le Logiciel Cisco IOS version 11.3 et est nécessaire pour distinguer IPSec et le chiffrement de propriété industrielle de Cisco fondent dans le Logiciel Cisco IOS version 11.2.`Loser#`**`show crypto cisco algorithms`** `des cfb-64 des cfb-8 40-bit-des cfb-64 40-bit-des cfb-8`
- **affichez le crypto clé-délai d'attente de Cisco** - Après qu'une session de communication chiffrée soit établie, elle est valide pour une durée spécifique. Après cette durée, les temps de session. Une nouvelle session doit être négociée, et une nouvelle clé DES (session) doit être générée pour que la transmission chiffrée continue. Utilisez cette commande de changer le temps qu'une session de communication chiffrée dure avant qu'elle expire (des périodes).`Loser#`**`show crypto cisco key-timeout`** `Session keys will be re-negotiated every 30 minutes` Utilisez ces commandes de déterminer la durée avant que les clés DES soient renégociées.`StHelen#`**`show crypto conn`** `Connection Table PE UPE Conn_id New_id Algorithm Time 0.0.0.1 0.0.0.1 4 0 DES_56_CFB64 Mar 01 1993 03:16:09 flags:TIME_KEYS StHelen#`**`show crypto key`** `Session keys will be re-negotiated every 30 minutes StHelen#`**`show clock`** `*03:21:23.031 UTC`

Mon Mar 1 1993

- **affichez les cryptos pregen-CAD-paires de Cisco** - Chaque session chiffrée utilise une seule paire de nombres CAD. Chaque fois qu'une nouvelle session est établie, de nouvelles paires de nombre CAD doivent être générées. Quand la session se termine, ces nombres sont jetés. Générer de nouvelles paires de nombre CAD est une activité CPU-intensive, qui peut faire la session installer lent, particulièrement pour des routeurs bas de gamme.Pour accélérer l'installation de session, vous pouvez choisir d'avoir une quantité spécifique de nombre CAD appareille précréé et tenu dans la réserve. Puis, quand une session de communication chiffrée est installée, une paire de nombre CAD est fournie de cette réserve. Après qu'une paire de nombre CAD soit utilisée, la réserve est automatiquement complétée le niveau avec une nouvelle paire de nombre CAD, de sorte qu'il y ait toujours des paires de nombre CAD opérationnelles.Il n'est habituellement pas nécessaire pour faire précréer plus d'un ou deux paires de nombre CAD, à moins que votre routeur installe des sessions chiffrées par multiple tellement fréquemment qu'une réserve précréée d'un ou deux paires de nombre CAD est épuisée trop rapidement.`Loser#`**`show crypto cisco pregen-dh-pairs`** `Number of pregenerated DH pairs: 10`
- **affichez le crypto active de connexions de Cisco**Voici un exemple de sortie de commande.`Loser#`**`show crypto engine connections active`** `ID Interface IP-Address State Algorithm Encrypt Decrypt 16 Serial1 19.19.19.19 set DES_56_CFB64 376 884`
- **affichez le crypto relâcher-paquet de connexions d'engine de Cisco**Voici un exemple de sortie de commande.`Loser#`**`show crypto engine connections dropped-packet`** `Interface IP-Address Drop Count Serial1 19.19.19.19 39`
- **configuration de show crypto engine** (était le **brief de show crypto engine** dans le Logiciel Cisco IOS version 11.2.)Voici un exemple de sortie de commande.`Loser#`**`show crypto engine configuration`** `slot: 0 engine name: fred engine type: software serial number: 02802219 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 465 input queue bot: 465 input queue count: 0`
- **DSS de mypubkey de show crypto key**Voici un exemple de sortie de commande.`Loser#`**`show crypto key mypubkey dss`** `crypto public-key fred 02802219 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit`
- **DSS de pubkey-chaîne de show crypto key**Voici un exemple de sortie de commande.`Loser#`**`show crypto key pubkey-chain dss`** `crypto public-key barney 05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341 quit`
- **affichez l'interface série 1 d'interface de crypto map**Voici un exemple de sortie de commande.`Loser#`**`show crypto map interface serial 1`** `Crypto Map "oldstyle" 10 cisco Connection Id = 16 (8 established, 0 failed) Peer = barney PE = 40.40.40.0 UPE = 30.30.30.0 Extended IP access list 133 access-list 133 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255` Notez la disparité de temps quand vous utilisez la **commande ping**.`wan-5200b#`**`ping 30.30.30.30`** `Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms wan-5200b# ----------- wan-5200b#`**`ping 30.30.30.31`** `Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms ----------------- wan-5200b#`**`ping 19.19.19.20`** `Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms ------------`
- **affichez l'interface série 1 d'interface de crypto map**Voici un exemple de sortie de commande.`Loser#`**`show crypto map`** `Crypto Map "oldstyle" 10 cisco Connection Id = 16 (8 established, 0 failed) Peer = barney PE = 40.40.40.0 UPE = 30.30.30.0 Extended IP access list 133 access-list 133 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255`
- **debug crypto engine**Voici un exemple de sortie de commande.`Loser#`**`debug crypto engine`** `Mar`

17 11:49:07.902: Crypto engine 0: generate alg param Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0 Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17 11:49:11.758: Crypto engine 0: generate alg param Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25 Mar 17 11:49:13.346: Crypto engine 0: verify signature Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25 Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25 Mar 17 11:49:24.946: Crypto engine 0: generate alg param

- **sessmgmt de debug crypto**Voici un exemple de sortie de commande.StHelen#**debug crypto sessmgmt** Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328, Found an ICMP connection message. Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19 Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0) Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0. Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0 Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK ~~ <---------- This is good ----------> ~~ Si le pair faux plaçait sur le crypto map, vous recevez ce message d'erreur.Mar 2 12:19:12.639: CRYPTO-SDU:Far end authentication error: Connection message verify failedSi les cryptos algorithmes ne s'assortissent pas, vous recevez ce message d'erreur.Mar 2 12:26:51.091: CRYPTO-SDU: Connection failed due to incompatible policySi la clé de DSS est manquante ou non valide, vous recevez ce message d'erreur.Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error: Connection message verify failed
- **clé de debug crypto**Voici un exemple de sortie de commande.StHelen#**debug crypto key** Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes. Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes. Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes. Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
- **effacez la crypto connexion**Voici un exemple de sortie de commande.wan-2511#**show crypto engine connections act** ID Interface IP-Address State Algorithm Encrypt Decrypt 9 Serial0 20.20.20.21 set DES_56_CFB64 29 28 wan-2511#**clear crypto connection 9** wan-2511# *Mar 5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0) *Mar 5 04:58:20.694: Crypto engine 0: delete connection 9 *Mar 5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK wan-2511# wan-2511#**show crypto engine connections act** ID Interface IP-Address State Algorithm Encrypt Decrypt wan-2511#
- **crypto mise à zéro**Voici un exemple de sortie de commande.wan-2511#**show crypto mypubkey** crypto public-key wan2511 01496536 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F quit wan-2511#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. wan-2511(config)#crypto zeroize Warning! Zeroize will remove your DSS signature keys. Do you want to continue? [yes/no]: **yes** % Keys to be removed are named wan2511. Do you really want to remove these keys? [yes/no]: **yes** % Zeroize done. wan-2511(config)#**^Z** wan-2511# wan-2511#show crypto mypubkey wan-2511#
- **aucune crypto clé publique**Voici un exemple de sortie de commande.wan-2511#**show crypto pubkey** crypto public-key wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit wan-2511#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. wan-2511(config)#**crypto public-key ?** WORD Peer name wan-2511(config)# wan-2511(config)#**no crypto public-key wan2516 01698232** wan-2511(config)#**^Z** wan-2511# wan-

```
2511#show crypto pubkey wan-2511#
```

Dépannage du Cisco 7200 avec l'ESA

Cisco fournit également une option d'aide de matériel de faire le chiffrement sur le Routeurs de la gamme Cisco 7200, qui s'appelle l'ESA. L'ESA est sous forme d'adaptateur de port pour la carte VIP2-40 ou d'adaptateur autonome de port pour le Cisco 7200. Cette organisation permet l'utilisation d'un adaptateur de matériel ou de l'engine du logiciel VIP2 de chiffrer et déchiffrer les données qui entrent dans ou partent par les interfaces sur la carte du Cisco 7500 VIP2. Le Cisco 7200 permet à l'aide de matériel pour chiffrer le trafic pour toutes les interfaces sur le châssis de Cisco 7200. Utilisant le cryptage une aide enregistre les cycles CPU précieux qui peuvent être utilisés à d'autres fins, comme le routage ou l'un des d'autres fonctions de Cisco IOS.

Sur un Cisco 7200, l'adaptateur autonome de port est configuré exactement les mêmes que le moteur de chiffrement de logiciel de Cisco IOS, mais a quelques commandes supplémentaires qui sont seulement utilisées pour le matériel et pour décider quelle engine (matériel ou logiciel) fera le cryptage.

D'abord, préparez le routeur pour le chiffrement matériel :

```
wan-7206a(config)#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
*Mar  2 08:17:16.739: ...switching to SW crypto engine

wan-7206a#show crypto card 3 Crypto card in slot: 3 Tampered: No Xtracted: Yes Password set: Yes
DSS Key set: Yes FW version 0x5049702 wan-7206a# wan-7206a(config)# wan-7206a(config)#crypto
zeroize 3 Warning! Zeroize will remove your DSS signature keys. Do you want to continue?
[yes/no]: yes % Keys to be removed are named hard. Do you really want to remove these keys?
[yes/no]: yes [OK]
```

Chiffrement matériel d'enable ou de débronchement comme affiché ci-dessous :

```
wan-7206a(config)#crypto esa shutdown 3 ...switching to SW crypto engine wan-
7206a(config)#crypto esa enable 3 There are no keys on the ESA in slot 3- ESA not enabled.
```

Ensuite, générez les clés pour l'ESA avant que vous l'activiez.

```
wan-7206a(config)#crypto gen-signature-keys hard % Initialize the crypto card password. You will
need this password in order to generate new signature keys or clear the crypto card extraction
latch. Password: Re-enter password: Generating DSS keys .... [OK] wan-7206a(config)# wan-
7206a#show crypto mypubkey crypto public-key hard 00000052 EE691A1F BD013874 5BA26DC4 91F17595
C8C06F4E F7F736F1 AD0CACEC 74AB8905 DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623
DCCE7322 3D97B804 quit wan-7206a# wan-7206a(config)#crypto esa enable 3 ...switching to HW
crypto engine wan-7206a#show crypto engine brie crypto engine name: hard crypto engine type: ESA
serial number: 00000052 crypto engine state: installed crypto firmware version: 5049702 crypto
engine in slot: 3 wan-7206a#
```

Dépannage de VIP2 avec l'ESA

L'adaptateur de port de matériel ESA sur la carte VIP2 est utilisé pour chiffrer et déchiffrer les données qui entrent dans ou partent par les interfaces sur la carte VIP2. Comme avec le Cisco 7200, utilisant une aide de cryptage enregistre les cycles CPU précieux. Dans ce cas, la **crypto** commande d'**enable esa** n'existe pas parce que l'adaptateur de port ESA fait le cryptage pour les ports sur la carte VIP2 si l'ESA est branché. **Le crypto clair-verrou** doit être appliqué à cet emplacement si l'adaptateur de port ESA était juste installé pour la première fois, ou a retiré alors réinstallé.

```
Router#show crypto card 11 Crypto card in slot: 11 Tampered: No Xtracted: Yes Password set: Yes
```

```
DSS Key set: Yes FW version 0x5049702 Router#
```

Puisque le crypto module ESA a été extrait, vous recevrez le message d'erreur suivant jusqu'à ce que vous fassiez une **crypto** commande de clair-**verrou** sur cet emplacement, comme affiché ci-dessous.

```
----
*Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed.
-----
Router(config)#crypto clear-latch ? <0-15> Chassis slot number Router(config)#crypto clear-latch
11 % Enter the crypto card password. Password: Router(config)#^Z
```

Si vous oubliez un mot de passe précédemment assigné, utilisez la **crypto** commande de **mise à zéro** au lieu de la **crypto** commande de clair-**verrou** de remettre à l'état initial l'ESA. Après avoir émis la **crypto** commande de **mise à zéro**, vous devez régénérer et des clés de DSS de re-échange. Quand vous régénérez des clés de DSS, vous êtes incité à créer un nouveau mot de passe. Un exemple est affiché ci-dessous.

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show crypto card 11 Crypto card in slot: 11 Tampered: No Xtracted: No Password set: Yes
DSS Key set: Yes FW version 0x5049702 Router# ------------------------------------------------
- Router#show crypto engine brief crypto engine name: TERT crypto engine type: software serial
number: 0459FC8C crypto engine state: dss key generated crypto lib version: 5.0.0 crypto engine
in slot: 6 crypto engine name: WAAA crypto engine type: ESA serial number: 00000078 crypto
engine state: dss key generated crypto firmware version: 5049702 crypto engine in slot: 11
Router# ----------- Router(config)#crypto zeroize Warning! Zeroize will remove your DSS
signature keys. Do you want to continue? [yes/no]: yes % Keys to be removed are named TERT. Do
you really want to remove these keys? [yes/no]: yes % Zeroize done. Router(config)#crypto
zeroize 11 Warning! Zeroize will remove your DSS signature keys. Do you want to continue?
[yes/no]: yes % Keys to be removed are named WAAA. Do you really want to remove these keys?
[yes/no]: yes [OK] Router(config)#^Z Router#show crypto engine brief crypto engine name: unknown
crypto engine type: software serial number: 0459FC8C crypto engine state: installed crypto lib
version: 5.0.0 crypto engine in slot: 6 crypto engine name: unknown crypto engine type: ESA
serial number: 00000078 crypto engine state: installed crypto firmware version: 5049702 crypto
engine in slot: 11 Router# -------------- Router(config)#crypto gen-signature-keys VIPESA 11 %
Initialize the crypto card password. You will need this password in order to generate new
signature keys or clear the crypto card extraction latch. Password: Re-enter password:
Generating DSS keys .... [OK] Router(config)# *Jan 24 01:39:52.923: Crypto engine 11: create key
pairs. ^Z Router# ------ Router#show crypto engine brief crypto engine name: unknown crypto
engine type: software serial number: 0459FC8C crypto engine state: installed crypto lib version:
5.0.0 crypto engine in slot: 6 crypto engine name: VIPESA crypto engine type: ESA serial number:
00000078 crypto engine state: dss key generated crypto firmware version: 5049702 crypto engine
in slot: 11 Router# ---------- Router#show crypto engine connections active 11 ID Interface IP-
Address State Algorithm Encrypt Decrypt 2 Serial11/0/0 20.20.20.21 set DES_56_CFB64 9996 9996
Router# Router#clear crypto connection 2 11 Router# *Jan 24 01:41:04.611: CRYPTO: Replacing 2 in
crypto maps with 0 (slot 11) *Jan 24 01:41:04.611: Crypto engine 11: delete connection 2 *Jan 24
01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK Router#show crypto engine
connections active 11 No connections. Router# *Jan 24 01:41:29.355: CRYPTO ENGINE:Number of
connection entries received from VIP 0 ------------ Router#show crypto mypub % Key for slot 11:
crypto public-key VIPESA 00000078 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD
A87BF7FE 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508 quit
Router#show crypto pub crypto public-key wan2516 01698232 C5DE8C46 8A69932C 70C92A2C 729449B3
FD10AC4D 1773A997 7F6BA37D 61997AC3 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22
CFAAC1A8 9CE82985 quit Router# ---------- interface Serial11/0/0 ip address 20.20.20.21
255.255.255.0 encapsulation ppp ip route-cache distributed no fair-queue no cdp enable crypto
map test ! ---------- Router#show crypto eng conn act 11 ID Interface IP-Address State Algorithm
Encrypt Decrypt 3 Serial11/0/0 20.20.20.21 set DES_56_CFB64 761 760 Router# *Jan 24
01:50:43.555: CRYPTO ENGINE:Number of connection entries received from VIP 1 Router#
```

Informations connexes

- Configuration et dépannage du chiffrement de couche réseau Cisco IPSec et ISAKMP - Partie 2
- PAP DES 46-2 au National Institute of Standards and Technology (NIST)
- PAP 186 de DSS au National Institute of Standards and Technology (NIST)
- Les forums aux questions des laboratoires RSA au sujet du chiffrement d'aujourd'hui
- Normes de sécurité IETF
- Configurer le protocole de sécurité IKE
- Sécurité des réseaux de configuration d'IPSec
- Page d'assistance IPsec
- Support technique - Cisco Systems